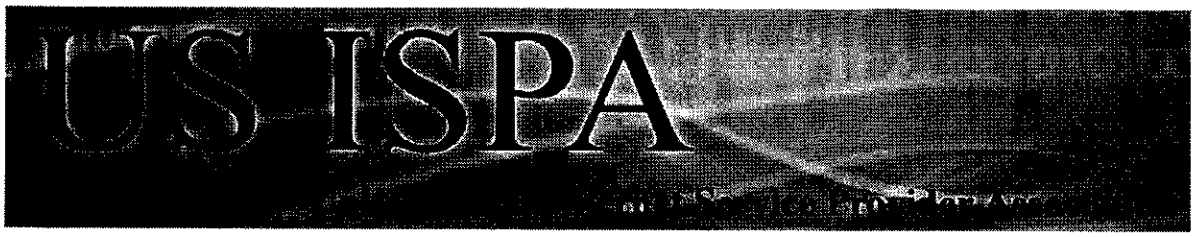
LATE TESTIMONY



January 26, 2012

The Honorable Angus McKelvey
Chairman
Committee on Economic Revitalization and Business
House of Representatives
State of Hawaii

Re: Opposition to HB 2288
Hearing: 8:30 a.m., January 26, 2012
Location: Hearing Room 312

Dear Chairman McKelvey:

Thank you for the opportunity to provide comment on HB 2288, a bill to require Internet service providers to retain customer records.

The United States Internet Service Provider Association ("US ISPA") is a national trade association that was founded ten years ago to focus on law enforcement compliance and security matters common to major Internet service, network and portal providers. Our membership includes AOL, AT&T, Comcast, Earthlink, United Online, Verizon and Yahoo!.

With our focus on law enforcement compliance issues, it is only natural that US ISPA members are interested in discussing data retention. We have participated in numerous efforts seeking to address data retention, including extensive dialogues with the Department of Justice, the National Association of Attorneys General, state and local law enforcement, and the privacy and civil liberties communities, and we have provided testimony before the United States Congress. As such, US ISPA is uniquely positioned to comment on HB 2288 and we welcome this opportunity to present our view to your committee.

Mandatory data retention presents complex challenges and risks

US ISPA has carefully examined past, more narrowly drafted, data retention proposals and each time has concluded that a uniform retention mandate is certain to present enormous

U.S. Internet Service Provider Association
700 12th Street, NW Suite 700
Washington, DC 20005
(p) +1.202.904.2351 www.usispa.org

challenges to the Internet service provider (ISP) industry. These challenges include regulatory burdens, technical complications, significant capital and expense costs, and diversion of capital from innovation. HB 2288 raises all of these concerns.

HB 2288 is over-broad and raises myriad privacy concerns

Data retention as mandated by HB 2288 would require an entire industry to retain billions of discrete electronic records: records tracking every Internet user's online activities, every online movement. The requirements of HB 2288 go far beyond the data retention legislation currently pending in the U.S. Congress, and well beyond the information which law enforcement would need to conduct investigations into the majority of online criminal activity. The scope of the data retention requirements under HB 2288 are dramatically disproportionate to the utility of the data that would be collected. The impact on consumer privacy of such a mandate is clear.

From a practical perspective, the sheer volume of data makes the task of gathering, storing and retrieving such data impracticable. Many providers have hundreds of thousands of users, some millions, and others hundreds of millions. By requiring ISPs to retain "each subscriber's information and Internet destination history," including IP addresses, domain names and host names, the bill would force companies to retain a broad swath of private data about consumers, their private communications, location and web-surfing activity. This creates serious constitutional concerns and the very real expectation of legal challenges.

The mandate would disproportionately burden Hawaii's local ISPs

HB 2288 would reach beyond Hawaii's borders and apply to many companies offering Internet access service across the nation and the costs to comply with this new law would greatly affect small and local Hawaiian ISPs. Smaller companies do not have the operational resources and capital held by their larger, national competitors. As a result, these regulations divert capital to data retention and away from other uses.

We do not have a cost estimate in dollars to propose to the Committee due to the sheer breadth of the legislation, but in looking at much narrower, national proposals in the past, US ISPA has estimated that narrower requirements would cost our membership well over $500 million in short-term compliance costs. Members of the Committee should carefully take into account the financial impact of HB 2288 on all providers, especially local Hawaiian companies, and consider whether such companies can absorb the compliance costs that will inevitably flow from the onerous data retention requirements in the bill.

Powerful tools for law enforcement already exist

Law enforcement has long had mechanisms at its disposal to preserve electronic evidence that might be useful for criminal or civil investigations. Use of these tools is far preferable from the industry's perspective than the imposition of burdensome data retention requirements.

U.S. Internet Service Provider Association
700 12th Street, NW Suite 700
Washington, DC 20005
(p) +1.202.904.2351 www.usispa.org

The preservation authority in the Stored Communications Act (18 U.S.C. § 2701 *et seq.*) was enacted into law in 1996 and has been used in a wide range of criminal investigations ever since. Section 2703(f) allows law enforcement, including state and local law enforcement, by letter, fax, or email to direct ISPs to preserve records and other electronic evidence in their possession pending the issuance of appropriate legal process. Upon request, providers must retain the records requested for up to 180 days. Thus, today, information and evidence believed to be important to a law enforcement investigation can be ***preserved*** without the requirement to issue formal legal process or even demonstrate relevance.

Preservation authority is a powerful, targeted tool available to law enforcement today that, from the perspective of US ISPA's members, strikes the appropriate balance between the government's legitimate need to preserve evidence for a pending investigation and the avoidance of undue burden on ISPs or consumer privacy.

In Conclusion

US ISPA remains committed to continuing a dialogue with policymakers and law enforcement about how we can contribute to the fight against online crime. We do not believe that a broad data retention requirement, such as that in HB 2288, is the right way to address the issue of cybercrime, however. Broad data retention mandates raise serious questions about breadth, scope, duration, liability and costs – costs that go well beyond mere dollars. These costs include the impact on innovation, privacy, and the ability of ISPs to afford the investments in data retention that HB 2288 would impose. Finally, the data retention debate is presently taking place in the U.S. Congress, which we believe is the proper forum for discussion of an issue of such wide-spread policy importance and that carries with it such significant cost and compliance implications.

For all these reasons, US ISPA respectfully urges this Committee not to proceed with HB 2288.

We thank you for this opportunity to present US ISPA's views on this topic and look forward to continuing to work with the Committee Members and your staff on these issues.

Respectfully,

Kate Dean
Executive Director

U.S. Internet Service Provider Association
700 12th Street, NW Suite 700
Washington, DC 20005
(p) +1.202.904.2351 www.usispa.org

LATE TESTIMONY

HB2288

RELATING TO RECORDKEEPING

KEN HIRAKI
VICE PRESIDENT-GOVERNMENT AFFAIRS

HAWAIIAN TELCOM

January 26, 2012

Chair McKelvey and members of the House Economic Revitalization & Business Committee:

I am Ken Hiraki, testifying on behalf of Hawaiian Telcom on HB 2288 – Relating to Recordkeeping which requires internet service providers to keep consumer records for no less than two years.

Hawaiian Telcom is opposed to this measure.

Implementation and compliance of such a storage system will have a significant financial impact to our company. In addition, it will take at least a year to determine whether such a system can be developed. Moreover we have many concerns regarding privacy, international law, and security.

Based on the aforementioned, Hawaiian Telcom respectfully requests that this measure be held. Thank you for the opportunity to testify.

LATE TESTIMONY

TESTIMONY ON
H.B. 2288, RELATING TO RECORDKEEPING
By
JEANNINE SOUKI
ON BEHALF OF THE
STATE PRIVACY AND SECURITY COALITION

Rep. Angus L.K. McKelvey
Chair, House Committee on Economic Revitalization & Business
Hawaii State Capitol, Room 427
Honolulu, HI 96813
Thursday, January 26, 2012, 8:30 AM

Brief Overview: Because of enormous implementation problems, risks to the personal privacy of law-abiding Internet users, availability of far less intrusive measures that work in the overwhelming majority of cases, and because the federal government is currently studying the issue, the House Economic Revitalization & Business Committee should not approve H.B. 2288 or its proposed data retention mandate.

- The State Privacy and Security Coalition – a coalition of leading technology companies and trade associations – and its members appreciate the concerns motivating introduction of H.B. 2288, but are convinced that the bill's data retention mandate is the wrong approach and would have serious unintended consequences. Our members stand ready to work with Hawaii law enforcement on better approaches to pursuing online crime.

- Every state that has considered an ISP data retention mandate has rejected the idea. Maine, Colorado, Utah and Arizona all specifically considered the idea and rejected it. In fact, even if one state mandated data retention, it would have no effect on tracing users who live outside of the State, but would impose impractical mandates on the state's local economy.

- What is more H.B. 2288 is far broader than any of these bills and than the federal data retention bill, H.R. 1981, pending in Congress. It requires retention of an unspecified range of "subscriber information", IP assignment data *and* domain and host name web destination data. This is a very large amount of information. It is both impractical for Hawaii businesses that provide Internet access to manage and, as I will discuss shortly, intrusive of privacy.

- Retention of IP address assignment data and web destination information is far from the only source of proof to identify suspects in online investigations. A much more flexible tool is part of federal law. 18 U.S.C. 2703(f) of the Stored Communications Act gives law enforcement authorities the power, with a simple written request, to require the preservation of any sort of electronic evidence by an electronic communications service provider (including an ISP). In fact, the marginal benefit from mandating retention of IP address and web destination information is far outweighed by the impracticability, negative privacy implications and constitutional uncertainties raised by a state mandate.

- The bill appears to assume that IP addresses correlate to individual subscribers. This is no longer the case. Indeed, on wireless networks, IP address assignments often change with each cell tower a user approaches. Furthermore, with an increasing number of landline ISPs, multiple customers will share the same IP address, through NAT router systems described in detail in the Center for Democracy & Technology's written testimony. Thus, the assumption that with the IP address assignment data retained, law enforcement will be able to find a particular Internet user is increasingly false.

- At the same time, a data retention mandate would raise significant risks to Hawaiians' privacy by requiring Internet access providers to store a huge range and volume of information regarding user movements on the Internet for two years. .

    - *Overwhelmingly affects innocent Internet users.* Think about this for a moment – would you want all the Internet domains you visited to be kept for two years and tied to your name? Requiring retention of "subscriber information", IP address assignment data, and destination domains and host names for all Internet users would have primarily affect the 99.9+% of users who are of no interest to law enforcement.

    - *Highly overbroad.* The key difference between data retention mandates and data preservation authority that I described earlier is that *data retention mandates would apply to the data of everyone who uses the Internet in Hawaii,* not just of law enforcement suspects.

    - *Subject to subpoena and discovery in civil litigation and administrative investigations.* Mandating that these data be retained would serve as a magnet for a host of intrusive requests. Litigants in civil cases, such as divorce and employment cases, politically motivated lawsuits, and administrative investigations would be on notice that they could obtain this information from Hawaii ISPs, posing a very real threat to privacy.

- The requirement to preserve this very large volume of data would be impractical for Hawaii's economy. Hotels, cafes, and WiFi hotspots are all businesses that provide Internet access and would need to comply. As would rural ISPs and telcos. Even for larger ISPs, the requirement is impractical. Wireless ISPs could not comply, as they typically assign IP addresses for brief periods, continually recycle them with no users and are unable to go back and identify a specific IP address. Likewise, ISPs that use technologies such as dynamic IP address assignment, network-address translation, and similar high-volume addressing methods would face significant implementation obstacles and great difficulty attempting to comply with a data retention mandate.

- Further, data retention legislation would still not prevent sophisticated criminals from evading retention. To be effective, data retention legislation must encompass all access technologies and Internet services—but this will likely impose disproportionate implementation obstacles on free and low cost services. Criminals who are well aware that their activities are illegal would be on notice that they should hide migrate to access methods and online services that are far harder to trace. Many of them will likely move instead to services such as WiFi hotspot access points, neighbors' unsecured WiFi connections, anonymizer services and others, that are likely to be exempted from any legislation and are the least likely to hold even temporary basic logs of activity. Ironically, a state data retention mandate may actually make it harder to trace sophisticated Internet criminals.

- For all of the reasons above, we respectfully request that this Committee not approve H.B. 2288. Thank you for the opportunity to testify, and we appreciate your consideration of our concerns.

LATE TESTIMONY

Testimony

submitted by

James X. Dempsey
Vice President for Public Policy
Center for Democracy & Technology[1]

to the

Committee on Economic Revitalization and Business
Chair: The Honorable Rep. Angus McKelvey

regarding

H.B. 2288

I. Introduction

A data retention mandate would require companies in the Internet ecosystem to retain certain information about all their users so that it would be available when sought by the government in investigations.[2] Data retention bills have been proposed in the U.S. Congress since 2006 but have never made it to a floor vote because of concerns about effectiveness, cost, and privacy.

H.B. 2288 would impose a data retention mandate on any company that provides access to the Internet. The exact scope of the data that would be required to be retained under H.B. 2288 is unclear: The bill states that "[t]he required data for the consumer records shall include each subscriber's information and internet destination history information." When data retention is discussed, "subscriber information" often is assumed to include the Internet Protocol ("IP") address associated with the communications of a subscriber.

---

[1] The Center for Democracy & Technology is non-profit public interest organization. Based in Washington, DC and with an office in San Francisco, CA, CDT works to keep the Internet open, innovative, and free. With expertise in law, technology, and policy, CDT seeks practical solutions to the challenges of the digital age. CDT convenes a series of working groups that bring together Internet, communications and technology companies, trade associations, think tank, and advocacy groups from across the political and ideological spectrum for dialogue and consensus building.

[2] One stated use of this data is in identifying the source of child pornography. CDT has long worked to protect children in the online environment while at the same time also protecting Internet users' privacy and other civil liberties. See generally, "Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes," CDT testimony before the House Judiciary Committee's Subcommittee on Crime, Terrorism, and Homeland Security (January 2011) http://judiciary.house.gov/hearings/pdf/Morris01252011.pdf (hereinafter "CDT Testimony").

This testimony analyzes the costs that a data retention mandate would impose on Internet Service Providers (ISPs), mobile carriers and other businesses.[3] It specifically focuses on developments in Internet addressing practices that will make the costs of retaining just one kind of data – IP addresses -- much larger than previously understood. It also explains why, as a result of those same trends in address allocation, IP address data may no longer reliably identify individual end-user devices, thus reducing the usefulness of a data retention mandate.

First, we describe a major development in Internet addressing: ISPs are sharing Internet addresses among multiple customers, which means that IP addresses no longer uniquely identify the computers or other devices of Internet users. (This development, as we explain below, is especially pertinent to H.B. 2288, which seems premised on the assumption that IP addresses are still unique.) We then explain why this trend in IP address sharing means that a data retention mandate would require the collection of vastly larger quantities of data at considerably greater cost than may have been projected even several years ago. We next discuss how the costs of compliance with a data retention mandate would especially harm small ISPs, such as those that serve rural or less populated areas. Finally, this testimony examines the implications of H.B. 2288 for coffee shops, hotels, and other businesses, most if not all of which use address sharing when they provide Internet access for visitors or employees. These entities, if covered by a mandate, would be forced to either assume the huge costs of data retention alongside ISPs or forgo providing Internet connectivity altogether.

II. Changes underway in IP address sharing would render compliance with a data retention mandate extraordinarily expensive

The high capital and operating costs associated with data retention mandates have long been identified as barriers to legislation.[4] However, recent changes in technology will render such mandates even costlier than previously anticipated.

First, some technical background: In the simplest configuration of Internet access, each device connected to the Internet is assigned a unique Internet Protocol address. The "IP

---

[3] In other memos and testimony, CDT has written extensively about the privacy implications of a data retention mandate. See, for example, CDT Testimony, note 2 above.

[4] Capital costs associated with data retention compliance include the costs of designing new collection and storage systems, purchasing collection and storage equipment, integrating new and existing systems, and developing systems to identify and deliver requested data to the government in a timely manner. Key operating costs associated with compliance include the costs of operating and maintaining interfaces for accessing the data in a timely manner, data security, compliance implementation staff, law enforcement liaison staff, staff training, system maintenance, and continuing system integration efforts. *See* Cable Europe, GSMA Europe, EuroISPA, ECTA (European Competitive Telecommunications Association), and ETNO (The European Telecommunications Network Operators' Association), Data Retention: Impact on Economic Operators (2009) at 1-2 (hereinafter "EU Joint Industry Statement"), available at https://www.vorratsdatenspeicherung.de/images/DRconsult/csp_joint_statement.pdf

address" of the device that is the source of a communication is associated with that communication as it is transmitted over the Internet. In some cases, the servers at the destination of the communication – for example, the servers that host the website the user is visiting or the instant messaging service being used – log the source IP addresses associated with each communication that they receive as well as the time of each communication. Government agents may obtain the source IP addresses and timestamps from these destination servers or by other means (such as by seizing and searching the computer of the recipient of the communication). With this information in hand, the government can often identify the ISP or mobile carrier that provided the sender's IP address, as publicly available records show which ISPs and mobile carriers use which blocks of IP addresses. The government can then ask the originating ISP or carrier to determine which customer was assigned the particular source IP address during the relevant time period.

Data retention legislation is intended to require ISPs and mobile carriers, and possibly other entities, to retain logs of the IP addresses they assign in order to be able to connect an IP address obtained by law enforcement at the end point of a communication to a particular customer at the communication's starting point.

H.B. 2288 seems to be premised on the simple configuration of Internet addressing described above. The bill defines Internet protocol address as "a numerical label assigned to each device participating in a computer network ... ."

Increasingly, however, ISPs are not using the simple configuration of Internet access described above. Instead, in a growing number of circumstances, IP addresses are being shared among many users, so that the IP address that passes over the Internet is no longer unique to a single end-user device. As we explain below, this change makes it complex and extraordinarily expensive for some ISPs to collect and retain the data necessary to retrospectively connect the source IP address as recorded at the end of a communication to an individual customer.

These changes are being driven by a critical shortage of traditional IP addresses, known as IPv4 addresses. In response to this shortage, key Internet stakeholders have embarked on a potentially decades-long transition to a new addressing protocol, known as IPv6. In the meantime, however, some major Internet access providers are adopting a very complex system of assigning IP addresses.

As a means of conserving IPv4 addresses, some ISPs and mobile carriers have adopted a technology known as Network Address Translation (NAT). NAT allows multiple Internet users to share the same IP address. Until recently, NAT was primarily used at a relatively small scale – for example, to have all of the devices within a single household or coffee shop share one address. However, because the pool of available IPv4 addresses is near exhaustion and the transition to IPv6 has only just begun, many ISPs and mobile carriers have begun or are planning to use NAT on a much larger scale. As a result, in some cases, a single IP address may be shared among thousands of customers. Furthermore, because devices that are only capable of understanding one version of IP or the other

need to communicate with each other during the transition phase, newer flavors of NAT have been developed to translate between IPv4 and IPv6.[5]

NAT usage, whether on a small or large scale, greatly increases the amount of data that must be stored in order to connect particular Internet activity to a specific customer. Below, we explain in more detail why NAT so drastically raises the costs of compliance with data retention mandates.

A. Many IP addresses no longer uniquely identify users or end-user devices

Whenever an Internet-connected device communicates on the public Internet, it is identified by a number called a public IP address, which is typically provided by the ISP or mobile carrier that connects that device to the Internet. Just as a street address sometimes identifies one unique individual, a public IP address sometimes identifies one unique Internet-connected device. However, just as a street address often identifies a multiple members of a family or even a large number of families and individuals, such as all those who live in the same apartment building, NAT allows a single public IP address to identify an entire household, all computers in an organization, or thousands of unrelated customers.

The way this works is that the ISP or carrier sets up a NAT router serving multiple users. Every device behind the router is assigned a private IP address, one that is not seen on the public Internet.[6] When one of these devices initiates a communication, the communication contains the source's private IP address and a number between 0 and 65,535 that is known as a port number.[7]

When the router behind which the device sits receives the source's private IP address and port number, it records them and then associates them with two new numbers: a public IP address that is possibly being used by many other devices sitting behind the same router and a port number that is not being used by any other device sitting behind the router. The ISP or mobile carrier uses what is known as a translation table (hence the name "Network Address Translation") to convert between the private IP address/port number

---

[5] This is a crucial detail, as machines that are IPv4 compatible and machines that are IPv6 compatible cannot easily communicate with each other. Consequently, ISPs must deploy transition technologies, such as NAT, to enable IPv4-capable devices and IPv6-capable devices to communicate with each other, and the use of such transition technologies will be necessary for the foreseeable future.

[6] This system allows ISPs and mobile carriers to use just one of their assigned public IP addresses to serve multiple customers, thus stretching the limited supply of IPv4 addresses assigned to the access providers.

[7] The port number is typically associated with the specific application or process initiating a communication, but the Internet protocol provides for so many port numbers (65,536 of them) that most of them are never used to identify an application. To facilitate IP address sharing, they have been re-purposed as device identifiers.

combination and the public one and thereby to ensure that the devices that share the same public IP address receive only the data intended for their devices.

Moreover, especially in the context of mobile Internet access, the IP address/port number combination for a particular device can change very frequently. Mobile devices can obtain a new IP address/port number combination as frequently as once every minute and possibly even more frequently.[8]

B. NAT complicates compliance with data retention mandates

Even for ISPs or mobile carriers whose networks use an IP address allocation scheme that does not involve NAT, compliance with a data retention mandate can be quite burdensome. IP addresses within these networks may change on a daily or weekly basis and – as we have discussed in past testimony, memos, and papers[9] – the high costs of retaining logs of these changes for six, twelve, or eighteen months can be quite burdensome.

For carriers and ISPs that deploy NAT, the cost and complexity of compliance with a data retention mandate would be especially burdensome. For some networks, new port assignments can occur as often as once every minute.[10] Depending on the type of NAT used, new data may need to be added to the ISP or carrier's logs each time a new port assignment occurs. This data includes a timestamp, outgoing port number, public and private IP addresses, and a link to the customer's identifying information. For a small or medium size ISP, this may amount to a data storage requirement on the order of terabytes of data per day. Under a data retention mandate, ISPs would be required not only to retain this data but also to have the capability to sift through it to satisfy a government demand. (Imagine re-issuing a copy of the White Pages as often as once a minute but still having to maintain all of the old copies.)

As the IPv4 address shortage becomes increasingly severe and the transition to IPv6 progresses, NAT may see even larger-scale deployment. Ensuring end-user identity with the complexities posed by NAT would require a mandate imposing extensive and expensive recordkeeping requirements on a wide range of entities.

---

[8] M. Balakrishnan, I. Mohomed, and V. Ramasubramanian, "Where's that Phone? Geolocating IP Addresses on 3G Networks," The Proceedings of the 2009 Internet Measurement Conference (Chicago, Illinois: Nov. 2009), *available at* http://research.microsoft.com/en-us/um/people/maheshba/papers/ephemera-imc09.pdf (hereinafter "Geolocating IP Addresses").

[9] Erica Newland and Cynthia Wong, "Data Retention Mandates: A Threat to Privacy, Free Expression, and Business Development," Center for Democracy & Technology, Oct. 2011, http://cdt.org/files/pdfs/CDT_Data_Retention_Paper.pdf; John Morris, Greg Nojeim, and Erica Newland, Memorandum on the Data Retention Mandate in H.R. 1981, Center for Democracy & Technology (July 19, 2011), http://www.cdt.org/files/pdfs/CDT_Letter_HR1981.pdf; CDT Testimony, note 2 above.

[10] Geolocating IP Addresses, note 8 above.

C. NAT adds to the already high costs of data retention

H.B. 2288 would require the retention not only of IP addresses but also "Internet destination history information." We are not aware of any cost estimates of such a mandate, since recent federal proposals have focused only on requiring retention of IP addresses. In this testimony, we focus only on IP address retention.

At the federal level, the Congressional Budget Office found that a data retention mandate would impose large up front costs on ISPs.[11] However, it does not appear that the CBO accounted for the added cost introduced by the wider adoption of NAT by ISPs and mobile carriers. Industry representatives, pointing to the new paradigm created by the addressing shortage and transition, have offered far higher estimates of the cost of complying with a data retention mandate.[12] Directly relevant to Hawaii, one small ISP with under 5 million subscribers has told CDT that it could face operating costs of $50 million per year, not including initial capital expenses incurred for the purchase of new equipment and the development of new systems for storing and accessing data. Moreover, in the words of the US ISP Association, cost estimates do not typically account for the "opportunity costs of having [ISPs' technical] experts diverted away from focus on innovating the next generation of Internet-based services."[13]

Finally, the difficulty of retrieving the information sought by the government in a timely manner cannot be overstated. Large-scale data storage increases the likelihood of system crashes and failures; the greater the volume of stored data, the less reliable the integrity of the data and the longer the delays when ISPs respond to demands from government. As the US ISP Association explained in testimony in January 2011, data retention may delay responses in true emergencies because of the slow speed of searching through massive volumes of data.[14] As NAT dramatically increases the volume of data that would be retained, it would also increase the likelihood of delays, errors and crashes.

D. Address sharing reduces the usefulness of data retention mandates

The idea of a data retention mandate was premised on the assumption that an IP address is a reliable Internet identifier. However, with address sharing, to make a match, it is

---

[11] CONG. BUDGET OFFICE, COST ESTIMATE FOR H.R. 1981 at 1 (Oct. 12, 2011).

[12] U.S. House, Committee on the Judiciary. *Protecting Children from Internet Pornographers Act of 2011.* (H. Rpt. 112-281). http://www.gpo.gov/fdsys/pkg/CRPT-112hrpt281/pdf/CRPT-112hrpt281-pt1.pdf.

[13] Written Testimony of Kate Dean (United States Internet Service Provider Association) before the House Committee on the Judiciary, Subcommittee on Crime, Terrorism and Homeland Security on "Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes," Jan. 25, 2011 (hereinafter "US ISPA Testimony"). *See also* EU Joint Industry Statement, note 4 above ("Furthermore, operational costs are increased by dedicated staff. Often the most qualified engineers, who are being asked to deal with the requests for information from LEAs or to give evidence in Court, are the most expensive and demanded resources.")

[14] US ISPA Testimony, note 13 above.

necessary to know not only the IP address associated with a communication, but also the port number and timestamp. However, the port number information necessary to make a match in a NAT context may not be logged at the destination point. Not all destination servers currently record incoming port numbers and for some it may be difficult or impossible to configure them to do so.

To make a match using NAT tables also requires that the clock used at the destination point to set the timestamp associated with the communication of concern be synchronized with the clock of the originating ISP. However, clocks on the Internet are not perfectly synchronized.[15] If the clocks of the destination server and the Internet access provider are off, even by a few seconds, it may not be possible to make a reliable match, leading to disclosure of data on innocent persons. This can be a problem especially in the mobile context, where the IP address and port number combination for a particular device may change rapidly.

III. Data retention mandates especially burden small ISPs

Many parts of rural America receive broadband services from small ISPs, without which they would remain stuck with slow dial-up services, unable to take advantage of large amounts of the content and services offered through the Internet today. Rural ISPs often serve communities in which larger ISPs have not been willing to invest.

ISPs serving rural or sparsely populated areas typically operate with very small profit margins. The many capital and operational costs of data retention[16] – from the purchase of new equipment to the development of data security measures[17] and systems for retrieving data in response to government demands – would be especially difficult for these ISPs to absorb, especially because small ISPs may deploy NAT in a more complex or layered fashion than do the larger ISPs. The National Telecommunications Cooperative Association (NTCA), a trade association for small and rural telecommunications cooperatives,[18] estimates that complying with the data retention mandate found in H.R. 1981 would create capital costs for a typical rural broadband

---

[15] See, e.g., Paul Krzyzanowski, "Clock Synchronization" (2009) http://www.cs.rutgers.edu/~pxk/417/notes/content/08-clocks.pdf

[16] See note 4 above.

[17] In Europe, despite data security requirements that are written into the data retention law, small ISPs have found it difficult to appropriately secure data. A recent European Commission report found the high cost of implementing security rendered these providers "unable to implement top IT security solutions protecting [retained data.]". *See* Article 29 Data Protection Working Party, Report 01/2010 on the Second Joint Enforcement Action (July 13, 2010) at 6, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_en.pdf.

[18] These cooperatives are often customer owned and supported by the government's Universal Service Fund.

provider that amount to between 5 and 7.5% of its annual revenue.[19] Such a requirement would likely run some of these ISPs out of business, thereby reducing broadband deployment in the United States and exacerbating the digital divide.[20]

IV. Hotels, coffee shops, airports, airplanes, buses, parks, libraries, convention centers and a host of other access providers also use NAT

HB 2288 has an extremely broad definition of Internet service provider: "a company that provides access to the Internet." This could cover not only ISPs but also coffee shops, hotels, airports, and others that offer Internet access to visitors as well as any business that provides Internet access to its employees.

Coffee shops, hotels, convention centers, airports, buses, trains, airplanes, schools, libraries and other entities providing Internet access to users or visitors very likely use NAT technology to distribute IP addresses within their networks. (Indeed, the use of NAT by small establishments predates its adoption at the carrier level.) All of a coffee shop's customers, for example, may sit behind a NAT router with a single IP address. The same complications for data retention that NAT creates for mobile carriers and ISPs are created for the small coffee shop, the hotel, the bus, and the airport. In almost all these cases, whether covered by the bill or not, the public facing IP address passed through the Internet by these entities and recorded at a destination point will not be the IP address assigned to an individual end-user device. Even if a regular ISP were to keep a record of the Internet address assigned to its customer (the coffee shop, hotel, employer), that customer could run a NAT router providing Internet access simultaneously to dozens or even hundreds of other people.[21]

---

[19] National Telecommunications Cooperative Association (NTCA), "Dynamic IP Address Assignment and Tracking," 2011. The costs will vary for each ISP as each network is different. The quoted cost range is for two different models for compliance that NTCA considered. In developing its cost estimates, NTCA made various assumptions about rural telecommunication companies and their existing infrastructure, the need to fully upgrade new infrastructure, the cost of equipment, and the cost to send a technician to each subscriber location (if required under the compliance approach) . These assumptions should not be assumed to be accurate for every network. According to NTCA, the loans required to finance these capital investments would very often be provided by the USDA Rural Utilities Service. However, due to the stringent loan review processes that are in place to ensure the appropriate use of taxpayer dollars, the loan approval process can take up to two years.

[20] Letter from Shirley Bloomfield, CEO, National Telecommunications Cooperative Association to Rep. Lamar Smith, Chair (July 26, 2011)("Finally, the nation's 1,150 rural providers are small businesses that operate on thin margins and lack the economies of scale to absorb a large, sudden cost. The rural telecom industry bears little resemblance to the largest providers, but it is essential to connecting the entire country. NTCA members serve areas where there is no business case for service and others refuse to serve. If rural providers were to exit their markets there would typically be no provider ready to step in and provide the kind of area-wide service that the local and national economies rely on.").

[21] NAT can be layered on NAT. The bus or train that uses NAT may receive its service from a carrier that uses NAT.

HB 2288, if enacted, will have one of two results: small businesses like coffee shops will be covered and will be required to collect and maintain complex records and systems for associating the IP addresses they assign to customers with the public-facing data they pass to the Internet, or coffee shops, hotels and many hundreds of other establishments become a gaping hole in the coverage, and hence the effectiveness, of the legislation. For entities that were covered, the infrastructure needed to store months' worth of records about each customer's behavior would require substantial investment in expensive equipment: the NAT routers these establishments typically use are incapable of keeping persistent logs – they simply don't have the storage capacity. Compliance with a data retention mandate would require these businesses to discard their current equipment and purchase all new equipment at considerable cost. Under HB 2288, many small businesses would likely be unable to continue to offer Internet access.[22]

V. Conclusion

It is widely recognized that a data retention mandate would have serious privacy consequences. Retained information would be available to the government for purposes other than those that prompted introduction of the legislation. Stored data could be vulnerable to hackers or to inadvertent disclosure. There is evidence that the data retention mandate in Europe has had a chilling effect on use of the Internet for provision of important services.[23] A data retention mandate is also likely to chill political use of the Internet and other free speech.

In this testimony, however, we focused on the costs of data retention and, to some extent, on its effectiveness in light of ongoing technological changes.

We recognize that ISPs and mobile carriers retain certain authentication data and certain IP address data for business purposes. Service providers are diligent in cooperating with government officials to provide whatever data they store. However, there is a world of difference between collecting and retaining data for business purposes and collecting, retaining and being able to retrieve that data for the purposes the government has in mind

---

[22] Regulatory burdens are, as a general matter, disproportionately borne by small businesses since they tend to be ill-equipped to absorb and comply with unfunded mandates. Nicole V. Crain and W. Mark Crain, *The Impact of Regulatory Costs on Small Firms*, U.S. Small Business Administration, Office of Advocacy (September 2010) at iv, *available at* http://archive.sba.gov/advo/research/rs371tot.pdf ("Small businesses . . . bear the largest burden of federal regulations. . . . [S]mall businesses face an annual regulatory cost . . . which is 36 percent higher than the regulatory cost facing large firms.").

[23] See Axel Arnbak, Plenary Presentation at the Taking on the Data Retention Directive Conference in Brussels: What the European Commission Owes 500 Million Europeans (Dec. 3, 2010) at 3, available at http://www.edri.org/files/Data_Retention_Conference_031210final.pdf (finding that as a result of a German data retention law, "half of Germans will not contact marriage counselors and psychotherapists" via e-mail), citing a German-language study by FORSA, "Opinions of citizens on data retention," June 2, 2008, available athttp://www.eco.de/dokumente/20080602_Forsa_VDS_Umfrage.pdf.

(uniquely identifying end-user devices). In this testimony, we have explained why that gap between business practices and a data retention mandate is growing even wider. Increasingly, the data retained for business purposes (at the beginning point of a communication, at the network level, and at the end points) is very different from the data that would have to be retained under a data retention mandate.

In the changing Internet ecosystem, data retention has become far more complex than even we at CDT understood several years ago. The evolution of IP address assignment practices has vastly increased the amount of data providers would have to retain in order to comply with H.B. 2288. Even with modern storage capabilities, the volume is so huge that the costs would be enormous, hurting especially small carriers serving rural communities, as well as coffee shops, hotels, and others that provide Internet access. This would slow or even reduce broadband deployment and divert financial and technical resources away from innovation.

Meanwhile, under current law, government already has the authority to require carriers to provide addressing data regarding specific accounts. State and local, as well as federal investigators in Hawaii have the authority, under 18 U.S.C. 2703(f), to require providers to preserve IP address and other information retrospectively on specific accounts. In addition, providers have a current obligation to preserve identifying information associated with child pornography that they find on their systems. These methods are highly effective in that they focus on specific users or accounts. These methods provide investigators with information relevant to a specific investigation and do not require the retention of massive amounts of information that will never be part of an investigation.

Mr. Chairman, members of the Committee, we appreciate the opportunity to submit this testimony. We would be happy to answer any further questions that you or your staff would have. Fell free to contact Jim Dempsey (jdempsey@cdt.org) at 415-814-1712.

LATE TESTIMONY

House Committee on Economic Revitalization and Business
January 26, 2012

From: Eliza Talbot

Re: Testimony in Support of HB 2288 Relating to Recordkeeping.

Chair McKelvey, Vice Chair Choy, and members of the ERB Committee,

Thank you for the opportunity to testify in support of HB 2288. I have personally seen and experienced the disturbing intrusion of internet harassment and bullying and believe current laws do not provide sufficient protection for victims. Because cybercrime is a recent phenomenon, in many cases Hawaii's penal code does not provide law enforcement the necessary authority to investigate and prosecute offenders.

This law will require internet service providers to retain costumer records for no less than 2 years. This simple change will provide crucial information to police officers investigating allegations of cybercrime and enable them to prosecute offenders.

Thank you for the opportunity to support this important legislation.

Mahalo,

Eliza Talbot

TESTIMONY **LATE TESTIMONY**

HB 2288 Relating to Recordkeeping

Date: Thursday, January 26, 2012

Time: 8:30 a.m.

Place: Conference Room 312, State Capitol, 415 South Beretania Street

Dear Committee Members:

We Oppose HB 2288

This bill incurs an unnecessary expense on ISPs which will no doubt be passed on to consumers.

A hacker with a small amount of skill is able to circumvent these records by launching the attack from an open wireless connection, or an internet café or, a compromised computer, all of which could be located anywhere on Earth.

Unintended consequences will surely result, such as abusing Hawaii residents who are only guilty of poor internet security practices.

Furthermore, these same techniques can be used to misdirect law enforcement to public figures such as the legislature or really anybody.

Thank you.

John Orendt

From: mailinglist@capitol.hawaii.gov
Sent: Wednesday, January 25, 2012 3:40 PM
To: ERBtestimony
Cc: phill@hookeletech.com
Subject: LATE TESTIMONY - Testimony for HB2288 on 1/26/2012 8:30:00 AM

Testimony for ERB 1/26/2012 8:30:00 AM HB2288

Conference room: 312
Testifier position: Oppose
Testifier will be present: No
Submitted by: Phill Moran
Organization: Individual
E-mail: phill@hookeletech.com
Submitted on: 1/25/2012

Comments:
The bill as written is erroneous and has no validity. Access to the data isn't covered, validation of the data is no possible.
The purpose of this bill is highly questionable - Why would the HI Government want to do this?
I strongly oppose.

From: mailinglist@capitol.hawaii.gov
Sent: Wednesday, January 25, 2012 5:00 PM
To: ERBtestimony
Cc: kdean@usispa.org
Subject: LATE TESTIMONY - Testimony for HB2288 on 1/26/2012 8:30:00 AM

Testimony for ERB 1/26/2012 8:30:00 AM HB2288

Conference room: 312
Testifier position: Oppose
Testifier will be present: No
Submitted by: Kate Dean
Organization: U.S. Internet Service Provider Association
E-mail: kdean@usispa.org
Submitted on: 1/25/2012

Comments:

From: Daniel Leuck [dan@ikayzo.com]
Sent: Wednesday, January 25, 2012 9:18 PM
To: ERBtestimony
Subject: Re: Testimony W/R to HB 2288

LATE TESTIMONY

Correction: In the second to last sentence I meant "warrant", not "subpoena". My corrected testimony:

Testifier: Daniel Leuck, CEO of Ikayzo, inc. (a Hawaii based software company)
Committee: COMMITTEE ON ECONOMIC REVITALIZATION & BUSINESS
Date & Time of Hearing: Thursday, January 26, 2012 at 8:30 a.m.
Regarding: HB 2288

Committee Members:

I wish to provide testimony with regard to HB 2288, which requires ISPs to capture and store all customer's internet traffic for a period of two years. In these times, the record of a person's browsing history is as close as you can get to a record of their thoughts. Even forcing telephone companies to record everyone's conversations, which is unthinkable, would be less of an intrusion. This bill represents a radical violation of privacy and opens the door to rampant fourth amendment violations. As with a phone tap, the state should be required to seek a warrant to record a person's browsing activities. Internet traffic can be far more personal than a phone call. Why should the protection of access be held to a lower bar?

Thank you for your time and attention.

On Wed, Jan 25, 2012 at 3:40 PM, Daniel Leuck <dan@ikayzo.com> wrote:
Testifier: Daniel Leuck, CEO of Ikayzo, inc. (a Hawaii based software company)
Committee: COMMITTEE ON ECONOMIC REVITALIZATION & BUSINESS
Date & Time of Hearing: Thursday, January 26, 2012 at 8:30 a.m.
Regarding: HB 2288

Committee Members:

I wish to provide testimony with regard to HB 2288, which requires ISPs to capture and store all customer's internet traffic for a period of two years. In these times, the record of a person's browsing history is as close as you can get to a record of their thoughts. Even forcing telephone companies to record everyone's conversations, which is unthinkable, would be less of an intrusion. This bill represents a radical violation of privacy and opens the door to rampant fourth amendment violations. As with a phone tap, the state should be required to seek a subpoena to record a person's browsing activities. Internet traffic can be far more personal than a phone call. Why should the protection of access be held to a lower bar?

Thank you for your time and attention.
--
Daniel Leuck
President
Ikayzo, inc.

From: mailinglist@capitol.hawaii.gov
Sent: Thursday, January 26, 2012 2:25 AM
To: ERBtestimony
Cc: danielwilsonhawaii@gmail.com
Subject: Testimony for HB2288 on 1/26/2012 8:30:00 AM

LATE TESTIMONY

Testimony for ERB 1/26/2012 8:30:00 AM HB2288

Conference room: 312
Testifier position: Oppose
Testifier will be present: No
Submitted by: Daniel R Wilson
Organization: Individual
E-mail: danielwilsonhawaii@gmail.com
Submitted on: 1/26/2012

Comments:

Dear Honorable State Representatives;
Would it be okay for the government to keep a record of the letters your mother sends and receives? Would it be okay for the government to keep a record of your daughter's email correspondence? Would it be okay for the government to listen to son's voicemail? Read your father's text messages? Listen to your own phone calls?
Why would it be okay for the government to mandate the generation of a dossier listing everywhere you go on the internet?
I do not understand the motivation for this bill. Many Americans have fought and died in wars to maintain our freedoms so why are the sponsors of this bill so keen to give them up? What pressing need here overwhelms our Fourth Amendment rights, our privacy? This broadly written, loosely defined bill would harm our personal freedom.
I strongly urge the house to not support the passing of HB2288. I'd be at the hearing to testify against it if I did I not have to work.
Sincerely,
Daniel Wilson
3798 Tantalus Drive

From: mailinglist@capitol.hawaii.gov
Sent: Thursday, January 26, 2012 4:07 AM
To: ERBtestimony
Cc: kathleen.klebba@gmail.com
Subject: Testimony for HB2288 on 1/26/2012 8:30:00 AM

LATE TESTIMONY

Testimony for ERB 1/26/2012 8:30:00 AM HB2288

Conference room: 312
Testifier position: Oppose
Testifier will be present: No
Submitted by: Kathleen Klebba
Organization: Individual
E-mail: kathleen.klebba@gmail.com
Submitted on: 1/26/2012

Comments:
Before I even mention the implications of recording and monitoring the internet activity of all Hawaii residents in order to (presumably) retain a few records used to subpoena a select few criminals, I'd like to say that, like SOPA (which was tabled for its obvious flaws), this bill's wording so broad that it could be applied businesses that provide internet access, which may affect Hawaii's tourist industry. As a former Hawaii resident and one who hopes to return in the future, I'm appalled that this bill would be introduced in its current form.

From: mailinglist@capitol.hawaii.gov
Sent: Thursday, January 26, 2012 6:39 AM
To: ERBtestimony
Cc: Kealii8@hotmail.com
Subject: Testimony for HB2288 on 1/26/2012 8:30:00 AM

LATE TESTIMONY

Testimony for ERB 1/26/2012 8:30:00 AM HB2288

Conference room: 312
Testifier position: Oppose
Testifier will be present: No
Submitted by: Kealii Makekau
Organization: Individual
E-mail: Kealii8@hotmail.com
Submitted on: 1/26/2012

Comments:
Rep. John Mizuno your election campaign mantra was that you WERE FOR THE PEOPLE, but now you introduce legislation that goes against the basic form of liberty and our first amendment right. With things such homelessness, inflation, economics still pending this bill is being fast track because of a sense of safety? I urge you to stick to your campaign promise and do right by the people for the people and strike this bill for consideration and address the real issues facing the people of Hawaii.

From: mailinglist@capitol.hawaii.gov
Sent: Thursday, January 26, 2012 6:44 AM
To: ERBtestimony
Cc: squide56@yahoo.com
Subject: Testimony for HB2288 on 1/26/2012 8:30:00 AM

LATE TESTIMONY

Testimony for ERB 1/26/2012 8:30:00 AM HB2288

Conference room: 312
Testifier position: Oppose
Testifier will be present: No
Submitted by: squide
Organization: Individual
E-mail: squide56@yahoo.com
Submitted on: 1/26/2012

Comments:
Are you kidding me?

LATE TESTIMONY

HOUSE COMMITTEE ON
ECONOMIC REVITALIZATION AND BUSINESS

January 26, 2012

House Bill 2288 Relating to Recordkeeping

Chair McKelvey and members of the House Committee on Economic Revitalization and Business, I am Rick Tsujimura, representing T-Mobile USA, Inc.

T-Mobile opposes House Bill 2288. This bill would require T-Mobile to retain IP address data, including the IP Address, Domain Name and Host name for every customer for 2 years. We oppose any bill requiring or imposing this kind of data retention requirement on wireless carriers because it is hugely burdensome for T-Mobile to implement. Our systems are not built to retain this data, and we don't currently store the IP address, nor do we really assign one. It would be astronomically expensive for T-Mobile to create such a system. The number of data traffic calls we manage annually could easily number in the billions, so building a system to track and maintain that much data would be more than problematic.

Not only does T-Mobile not currently store any IP address records, T-Mobile doesn't assign individual IP addresses to most users. T-Mobile doesn't have the number of IP addresses that would be required to do so, and our systems aren't designed to work that way.

It is critical that we all start with an understanding that - based on current technologies in use - in most cases the wireless carriers simply cannot return an identified name and address for a person associated with an IP address on a given date and time. Although we provide a service that allows access to the internet that may appear to operate much like the way wireline services are operated, the underlying technologies, routing, and record keeping is very different.

Wireless carriers generally do not allocate a unique public IP address to each individual user in the same way that wireline providers do.

- Instead, the wireless gateways generally use a very small number of public IP addresses that are shared by multiple users at any single point in time.

- As a general rule, carriers never create logs of the correlation between the specific content flowing between a user and the destination site. It is not required for business purposes and the systems were not engineered to attempt to keep track of this much information.

- More importantly, even if those logs were kept, the only address that is ever seen by the destination site is the shared public IP address.

- Thus, if law enforcement, for example, were undertaking an investigation and started with that public IP address, and traced it back to the wireless carrier, even if the wireless

carrier could technically keep the detailed private IP address logs, at most the carrier would only be able to respond by indicating all the users that were using the single public IP address at a given point in time. In other words, it would be a lot like Southwest being able to give you the entire passenger list of a flight, but unable to tell you which passengers specifically were assigned to or sitting in row 3.

For these reasons we oppose HB2288 and request that the bill be held or specifically exclude wireless carriers.

LATE TESTIMONY

The NetChoice Coalition
Promoting Convenience, Choice, and Commerce on The Net

Steve DelBianco, Executive Director
1401 K St NW, Suite 502
Washington, DC 20005
202-420-7482
www.netchoice.org

January 26, 2012

Representative Angus McKelvey
Chairman, Committee on Economic Revitalization and Business
House of Representatives
Hawaii State Capitol

RE: **Opposition to HB 2288, Data Retention Mandate**

Dear Chairman McKelvey:

NetChoice opposes HB 2288 which forces ISPs to create and retain an evidentiary trail for all Hawaiians who pay to access the Internet. This bill would enable government to investigate users' online activities – often without a warrant or court-ordered subpoena. This raises serious privacy concerns for customers of paid Internet services.

HB 2288 Creates a Real Threat to Hawaiian Privacy

Every time a Hawaiian accesses the Internet -- whether at home, in a hotel, in a coffee shop, or anywhere they use their smartphone – a unique IP address is assigned in order to connect that user to the web.

HB 2288 would require companies providing paid Internet access to retain a record of each IP address assigned for the last two years, and to link that IP address to webpages visited and the customer's identity.

HB 2288

Creates Threat to American Privacy

- Government Tracking of Honest Hawaiians
- Misuse of Data in Lawsuits
- Misuse of Data by Criminals

Undermines Federal and Congressional Privacy Initiatives

ISPs Already Work with Law Enforcement to Protect Citizens

Government Tracking of Honest Hawaiians

This bill would enable government to find out where a Hawaiian is located every time they check their email, go online with a smartphone, or pay to access the Internet in a hotel room or airport. HB 2288 would enable government to know which websites a Hawaiian has visited and where and when they traveled for the past two years. Forcing companies to store this for government use opposes the goals of the 4th and 5th Amendments to the Constitution: preventing the government from unlawful searches of citizens.

Misuse of Data in Lawsuits

The information that HB 2288 requires ISPs to collect could be misused in lawsuits. Attorneys could subpoena this information to build their cases. For example, an attorney in a divorce or child custody case could subpoena this data to discover someone's travels and the webpages they have visited. If a Hawaiian were researching medical information or seeking psychiatric help, that might be quite damaging in such a court proceeding.

Misuse of Data by Criminals

This repository of IP addresses with customer IDs creates a honey pot of consumer information that is susceptible to misuse. This misuse could occur through a data breach, employee theft, or a hacking episode. Data breaches are a real risk, so having all this user data stored in a few locations makes a very tempting target for criminals.

Undermines Federal and Business Privacy Initiatives

The Federal Trade Commission and the Department of Commerce have espoused the need for consumer choice in the tracking of their online activity. And each of these agencies expects to release privacy reports in the next few months.

Today, most Internet companies and web browsers already allow their customers to opt-out of having their web-surfing information tracked or stored. These policies recognize the consumer's right to maintain control over their information and are an important tool in securing user trust.

But HB 2288 would prevent these efforts to increase consumer choice by forcing ISPs to track their customers. By forcing ISPs to retain these IP addresses and the web pages accessed, the law would prohibit anonymous Internet browsing and undermine current government efforts to increase online privacy for Hawaiians.

ISPs Already Work with Law Enforcement to Protect Citizens

Existing efforts already achieve the goals of HB 2288. Current data preservation laws require all Internet services (both free and paid) to preserve all data pertaining to a customer when approached by law enforcement. This provides police with time to gather additional evidence and secure the necessary court orders to obtain the evidence preserved and retained by the ISP.

Moreover, when tracking illegal internet activity today, law enforcement is ten times more likely to ask ISPs for the person behind *an email address* or *chat name,* compared to requests for an IP address used to post something to a public website. ISPs already comply with all requests from law enforcement to preserve a specified user's IP connectivity logs. These processes more accurately reflect our justice system, where data is only collected on a potential criminal when they are *suspected* of a crime, rather than under HB 2288 where data is gathered on all Hawaiians *in case* they become a suspect in a crime.

LATE TESTIMONY

Free and paid Internet services have a strong and effective working relationship with law enforcement. This existing working relationship obfuscates the need for additional laws that will complicate this working process even further.

Today, law enforcement appears not to have sufficient resources to keep up with the volume of evidence being provided to them by ISPs. So it may be that governments could do more to pursue online crime by adding resources to existing law enforcement efforts.

HB 2288 Threatens Hawaiian Privacy

HB 2288 will threaten the privacy of Hawaiians by potentially exposing their information to criminals and private attorneys. Moreover, HB 2288 places honest Hawaiians under the scrutiny of their government.

Thank you for considering our views, and please let me know if we can provide further information.

Sincerely,

Steve DelBianco
Executive Director, NetChoice
cc: Members of Economic Revitalization & Business Committee

NetChoice is a coalition of trade associations and e-Commerce businesses who share the goal of promoting convenience, choice and commerce on the Net. More information about NetChoice can be found at www.netchoice.org

LATE TESTIMONY

From: mailinglist@capitol.hawaii.gov
Sent: Thursday, January 26, 2012 1:39 PM
To: ERBtestimony
Cc: hintzjason@yahoo.com
Subject: LATE LATE Testimony for HB2288 on 1/26/2012 8:30:00 AM
Attachments: HB 2288 Against.doc

Testimony for ERB 1/26/2012 8:30:00 AM HB2288

Conference room: 312
Testifier position: Oppose
Testifier will be present: No
Submitted by: Jason Hintz
Organization: Individual
E-mail: hintzjason@yahoo.com
Submitted on: 1/26/2012

Comments:

See attached

1

Jason Hintz

I, Jason Hintz, resident of Hawaii for 15 ½ years, am against House Bill 2288. The bill states that "internet destination history information" and "subscriber's information" such as name and address must be saved for two years. To put it simply, the state government will have internet providers create a file about everyone and list every website everyone visited in the past two years and attach those websites to our name.

What troubles me more is that the proposal is extremely broad and has no specifications whatsoever for privacy. There are no restrictions what internet providers can do (like selling our personal information to advertisers), no instructions stating that police need a court order to look at the files and no stipulation that the data must be encrypted.

This is an invasion of privacy and in direct violation of the 4th Amendment of the United States Constitution. The last time I checked, Hawaii is still part of the United States. Not only will passing this bill will strip Hawaii residents of their Constitutional rights, you'll be opening it to attacks by hackers such as Anonymous who no doubt will attack the government until the House Bill is no more. This bill is similar to SOPA and PIPA, which millions of Americans and corporations have protested against and which supporters were attacked by Anonymous.

Save yourself the trouble and kill this bill. This is one Pandora box you don't want to open.

LATE TESTIMONY

From: mailinglist@capitol.hawaii.gov
Sent: Thursday, January 26, 2012 12:46 PM
To: ERBtestimony
Cc: aaron.collinsa@gmail.com
Subject: LATE LATE Testimony for HB2288 on 1/26/2012 8:30:00 AM
Attachments: testimony.1-26-2012.doc

Testimony for ERB 1/26/2012 8:30:00 AM HB2288

Conference room: 312
Testifier position: Oppose
Testifier will be present: No
Submitted by: Aaron Collins
Organization: Hilo Hattie
E-mail: aaron.collinsa@gmail.com
Submitted on: 1/26/2012

See attached

Comments:

(1)

Aaron Collins

As a leading IT engineer in Hawaii I have to say I heavily oppose this bill in it's current form. This bill will be a significant violation of privacy and provide no benefit to law enforcement. The reality is that anyone who is going to commit a crime online is going to take precautions and use publicly available well known tools to hide their actions. (See: https://www.torproject.org)

I've worked in internet security for over a decade. In every security incident I've ever done forensic analysis on one common tactic I've seen is that the attackers always hide their IP. Keeping every citizens internet usage logs on the off chance that you might find one criminal that might of made a mistake is counter productive.

You also really need to take into account the significant amount of extra work and expenses you are going to put on Hawaii's local business. Adding this type of auditing on public wifi will cost each business at least $1500 in hardware and licensing alone to accomplish this task. This doesn't even take into account the manpower and labor cost. When you take into account how many business in Hawaii offer public wifi the cost is astounding.

As a security Engineer with over a decade of experience in these matters as well as the engineer who setup the State of Hawaii's online portal security, I strongly urge you to not pass this law. If cyber crime is this much of an issue here in Hawaii I recommend holding public forms to discuss this matter with Hawaii's leading technology professionals so we can work together to develop a true solution to cyber threats. I would be even willing to help organize this and offer recommendations.

Signed,

Aaron Collins

808.203.8756

aaron.collinsa@gmail.com

LATE TESTIMONY

From: mailinglist@capitol.hawaii.gov
Sent: Thursday, January 26, 2012 12:43 PM
To: ERBtestimony
Cc: ofeliahernandez@gmail.com
Subject: LATE LATE Testimony for HB2288 on 1/26/2012 8:30:00 AM
Attachments: HB2288.docx

Testimony for ERB 1/26/2012 8:30:00 AM HB2288

Conference room: 312
Testifier position: Oppose
Testifier will be present: No
Submitted by: Ofelia Hernandez
Organization: Individual
E-mail: ofeliahernandez@gmail.com
Submitted on: 1/26/2012

Comments:
Let's protect our freedom and not limit it.

see attached

(1)

Ofelia Hernandez

January 26, 2012

To whom it may concern:

I wish to express my stand on measure HB2288, which I oppose 100%. It seems like every day more of our freedom and basic rights are taken away and this measure is another tool to limit, censor and control us. As citizens we have the right to browse whatever websites we wish, it is a services we pay for and can utilize in the privacy of our homes. I do not feel it is necessary to keep track of my likes and dislikes through the websites I visit. While I understand some people abuse the internet and use it to commit illegal activity, this can be said in every aspect, for example how some politicians abuse their authority and use their power for useless legislation instead of working towards the improvement of Hawaii. I feel that is this measure is passed it is a direct violation of my rights and freedom. I hope that as a voting citizen, my opinion is taken into account.

Regards

Ofelia Hernandez

(2)

LATE TESTIMONY

From: mailinglist@capitol.hawaii.gov
Sent: Thursday, January 26, 2012 12:13 PM
To: ERBtestimony
Cc: michael.simao@yahoo.com
Subject: LATE LATE Testimony for HB2288 on 1/26/2012 8:30:00 AM
Attachments: Testimony.docx

Testimony for ERB 1/26/2012 8:30:00 AM HB2288

Conference room: 312
Testifier position: Oppose
Testifier will be present: No
Submitted by: Michael Simao
Organization: Individual
E-mail: michael.simao@yahoo.com
Submitted on: 1/26/2012

Comments:
Thank you for providing this forum for bringing our testimony to these hearings. I hope that my testimony will be considered with proper weight as being from a very concerned citizen of our island state.

See Attached

(1)

Michael Simao

To Whom It May Concern,

Upon hearing of the bill being proposed here in Hawaii regarding the retention of IP information, I have to admit that I was a little shocked, especially in light of the recent overwhelming disapproval with which the SOPA and PIPA bills were met. This bill constitutes a gross violation, or a potential gross violation, of our fourth and fifth amendment rights. Please let me stop here for a moment and clarify something. I am not pointing this out as a person who has any fear of discovery of illicit or illegal activity. I am, however, a person who respects the privacy of individuals and I believe that, with the nature in which the internet has filtered into every aspect of most people's lives, this bill would violate too many of our privacies. The government does not have the right to place cameras in every room of a person's house, but in some ways, this would be even more invasive, because many people share far more online than they do even within their own homes. Not only does this then become an issue of privacy, but also one of security. This bill is alleged to protect people from the violations of hackers and other internet predators out there, and I applaud the intent. However, there are too many ways in which something like this could turn out to be a greater threat to that security. For example, for a person to hack into someone's account, from my understanding of it, they first need to have information on who is going into an account somewhere. Now if every website I visit is being retained somewhere, what is to stop this predator from getting my retained information and using it to set up keyloggers or other tools to capture my information? Personally, I believe that internet security is the responsibility of the users as much as of any government entity, but this is irrelevant in the face of these other concerns. However, as I stated in the beginning of this letter, I am most concerned about privacy. I have no desire to allow anyone to snoop through what I do with my free time online, and I know that there are many, many others who feel the same. I would strongly recommend that this bill be put down, and the issue of internet security addressed in another way.

Thank you very much for your time and consideration and I pray that you will use this and other testimonies to determine the best outcome for this bill. My opinion on the subject is known.

Sincerely,

Michael Simao

LATE TESTIMONY

January 26, 2012

Honorable Members of the Committee,

I wish to express my opposition to HB2288 and offer some information that may help you make a decision.

I am a software engineer who has been working for the past dozen years on internet server software that transports user web traffic for internet service providers and wireless carriers (that is, the phone companies who carry the cellular traffic).

I have been involved in providing features that can track web requests, write them to disk and transport them off-device for analysis or storage. You might be interested to know that the results of this kind of collection on an active network can result in up to gigabytes of data per hour from a single device, and a major carrier would have many such devices.

HB2288 requires long term storage of this data, which cannot be done on the devices that transport the data. It must be picked up from analysis of the data stream, buffered, then written to some other device. Usually this involves transporting the data over the network again to some device with the storage capacity. This interferes with the usage of the network to carry customer requests and requires the ISP to purchase additional bandwidth and equipment.

Your committee may not be aware that when you fetch a web page with your browser, it's not just the initial page that is fetched and that would have to be recorded. To speed up browsing, you browser may pre-fetch pages that are referenced by links in the primary page. It will also fetch other content (images, banners, etc.) that are used to build the fetched page. Each of these images is seen as a separate web request that your bill would require storing. All of these images can, and usually do, come from different sites than the one you thought you were fetching. This is especially true of all the ads that come from ad server sites.

Besides being a massive invasion of the privacy of law abiding citizens, this bill would be a massive burden on internet service providers and would result in a reduction of service to customers due to (a) the collected information placing extra demand on the network and (b) the necessity to slow down the requests when the logging of destinations cannot keep up with the requests.

If law enforcement needs to track this kind of information, they should target individuals suspected of crimes and for whom they can get warrants, rather than creating a massive surveillance state of private citizens for their own convenience.

Thank you for your consideration.

John Hardin
1701 Hooli Street
Lahaina, HI 96761

LATE TESTIMONY

From: mailinglist@capitol.hawaii.gov
Sent: Thursday, January 26, 2012 11:39 AM
To: ERBtestimony
Cc: jkcabral77@gmail.com
Subject: LATE LATE Testimony for HB2288 on 1/26/2012 8:30:00 AM

Testimony for ERB 1/26/2012 8:30:00 AM HB2288

Conference room: 312
Testifier position: Oppose
Testifier will be present: No
Submitted by: Jason Cabral
Organization: Individual
E-mail: jkcabral77@gmail.com
Submitted on: 1/26/2012

Comments:

LATE TESTIMONY

From: mailinglist@capitol.hawaii.gov
Sent: Thursday, January 26, 2012 11:35 AM
To: ERBtestimony
Cc: daniel@contrastmagazine.com
Subject: LATE LATE Testimony for HB2288 on 1/26/2012 8:30:00 AM

Testimony for ERB 1/26/2012 8:30:00 AM HB2288

Conference room: 312
Testifier position: Oppose
Testifier will be present: No
Submitted by: Daniel Ikaika Ito
Organization: Individual
E-mail: daniel@contrastmagazine.com
Submitted on: 1/26/2012

Comments:
This bill is too broad to do any good, and is a serious invasion of our privacy with the potential for catastrophic repercussions on our rights.

LATE TESTIMONY

From: mailinglist@capitol.hawaii.gov
Sent: Thursday, January 26, 2012 11:24 AM
To: ERBtestimony
Cc: devinawong@mac.com
Subject: LATE LATE Testimony for HB2288 on 1/26/2012 8:30:00 AM

Testimony for ERB 1/26/2012 8:30:00 AM HB2288

Conference room: 312
Testifier position: Oppose
Testifier will be present: No
Submitted by: Devin Awong
Organization: Individual
E-mail: devinawong@mac.com
Submitted on: 1/26/2012

Comments:

LATE TESTIMONY

From: mailinglist@capitol.hawaii.gov
Sent: Thursday, January 26, 2012 11:23 AM
To: ERBtestimony
Cc: kipikoa1@hotmail.com
Subject: LATE LATE Testimony for HB2288 on 1/26/2012 8:30:00 AM

Testimony for ERB 1/26/2012 8:30:00 AM HB2288

Conference room: 312
Testifier position: Oppose
Testifier will be present: No
Submitted by: Steven Tayama
Organization: Nation of Hawaii
E-mail: kipikoa1@hotmail.com
Submitted on: 1/26/2012

Comments:
What could possibly be the purpose if this bill except to intrude on peoples privacy??!!This is something that would happen in Nazi Germany and not Hawaii! I say, Government STAY OUT OF OUR PRIVATE LIVES! Fix the roads and sewers. Improve our schools and parks. Build truly affordable housing and fix public housing. Here is a novel idea for government to focus on. Lessen our total dependency on barges bringing in everything we need and make us at least food independent.Stop this grand stand bill and get to real solutions!

LATE TESTIMONY

From: mailinglist@capitol.hawaii.gov
Sent: Thursday, January 26, 2012 11:23 AM
To: ERBtestimony
Cc: roxanne@barefeetstudios.com
Subject: LATE LATE Testimony for HB2288 on 1/26/2012 8:30:00 AM

Testimony for ERB 1/26/2012 8:30:00 AM HB2288

Conference room: 312
Testifier position: Oppose
Testifier will be present: No
Submitted by: Roxanne Darling
Organization: Individual
E-mail: roxanne@barefeetstudios.com
Submitted on: 1/26/2012

Comments:
This bill is poorly drafted, will not stop internet crime, and seriously violates personal privacy for residents and tourists alike. It further creates an extraordinary burden on internet service providers and should be stopped immediately. I respectfully request the committee withdraw it, consult with technical and legal experts who understand how the internet and the constitution work, and then we can all happily re-visit it. I would also like to know exactly who proposed this legislation, why, and when. That is very relevant information in my opinion.

LATE TESTIMONY

From: mailinglist@capitol.hawaii.gov
Sent: Thursday, January 26, 2012 11:18 AM
To: ERBtestimony
Cc: djobe@hawaii.edu
Subject: LATE LATE Testimony for HB2288 on 1/26/2012 8:30:00 AM

Testimony for ERB 1/26/2012 8:30:00 AM HB2288

Conference room: 312
Testifier position: Oppose
Testifier will be present: No
Submitted by: Donald
Organization: Individual
E-mail: djobe@hawaii.edu
Submitted on: 1/26/2012

Comments:
I find, this tracking of personal data, unneeded and unwarranted. This amounts to unlawful searching of peoples private lives.

LATE TESTIMONY

From: mailinglist@capitol.hawaii.gov
Sent: Thursday, January 26, 2012 11:07 AM
To: ERBtestimony
Cc: carl.sholin@gmail.com
Subject: LATE LATE Testimony for HB2288 on 1/26/2012 8:30:00 AM
Attachments: HB2288_CSholinTestimony.doc

Testimony for ERB 1/26/2012 8:30:00 AM HB2288

Conference room: 312
Testifier position: Oppose
Testifier will be present: No
Submitted by: Carl Sholin
Organization: Individual
E-mail: carl.sholin@gmail.com
Submitted on: 1/26/2012

Comments:

Hello, My name is Carl Sholin and I have been a resident of the state of Hawaii for the past 2 1/2 years; I currently live in the Hawaii State 28th Congressional District and the Hawaii State Senate District 11. I would like to voice my opposition to House Bill 2288. To my knowledge a bill of this nature is unprecedented in the United States. This bill is highly invasive for both an individuals' privacy and for the privacy of businesses in the state of Hawaii. I am very disturbed that the State of Hawaii would feel a need to have surveillance on all its residents and visitors. I see this bill as a gross invasion of individual privacy.

LATE TESTIMONY

From: mailinglist@capitol.hawaii.gov
Sent: Thursday, January 26, 2012 11:00 AM
To: ERBtestimony
Cc: stefan@metawerks.net
Subject: LATE LATE Testimony for HB2288 on 1/26/2012 8:30:00 AM

Testimony for ERB 1/26/2012 8:30:00 AM HB2288

Conference room: 312
Testifier position: Oppose
Testifier will be present: No
Submitted by: Stefan Odum
Organization: Individual
E-mail: stefan@metawerks.net
Submitted on: 1/26/2012

Comments:
HB2288 should be voted down for the fact that it is an unprecedented attempt access to personal information and is a severe blow to privacy, both for individuals and business. The collection of this kind of data can be used two ways, data mining for profit and for surveillance. The government should not be allowed to record this personal information as a means of surveillance, even if it requires a warrant to access it. As the measure is written now, it does not contain any language or estimate regarding to the cost of storing such vast amount of information. How can we appropriate funds for this? Will the burden of the cost fall on the ISP, who then will pass along the cost to the consumer? The measure doesn't have any language protecting the stored data from third parties accessing the data, or requiring encryption of the stored data which in itself a serious privacy concern.

Please protect our privacy and vote NO on this measure.

LATE TESTIMONY

From: mailinglist@capitol.hawaii.gov
Sent: Thursday, January 26, 2012 10:51 AM
To: ERBtestimony
Cc: jmphee@gmail.com
Subject: LATE LATE Testimony for HB2288 on 1/26/2012 8:30:00 AM

Testimony for ERB 1/26/2012 8:30:00 AM HB2288

Conference room: 312
Testifier position: Oppose
Testifier will be present: No
Submitted by: James Phee
Organization: Individual
E-mail: jmphee@gmail.com
Submitted on: 1/26/2012

Comments:
This is an absolutely horrible bill that violates the Fourth Amendment in so many ways. The fact that Rep Mizuno or any elected official could suggest such a massively privacy-violating measure is a slap in the face to the citizens he's supposed to serve.

LATE TESTIMONY

From: mailinglist@capitol.hawaii.gov
Sent: Thursday, January 26, 2012 10:43 AM
To: ERBtestimony
Cc: hstilmack@gmail.com
Subject: LATE LATE Testimony for HB2288 on 1/26/2012 8:30:00 AM

Testimony for ERB 1/26/2012 8:30:00 AM HB2288

Conference room: 312
Testifier position: Oppose
Testifier will be present: No
Submitted by: Henry Stilmack
Organization: Individual
E-mail: hstilmack@gmail.com
Submitted on: 1/26/2012

Comments:

LATE TESTIMONY

From: mailinglist@capitol.hawaii.gov
Sent: Thursday, January 26, 2012 10:21 AM
To: ERBtestimony
Cc: webmaster@hawaiitalks.net
Subject: LATE LATE Testimony for HB2288 on 1/26/2012 8:30:00 AM
Attachments: opposetestimonyHB2288.pdf

Testimony for ERB 1/26/2012 8:30:00 AM HB2288

Conference room: 312
Testifier position: Oppose
Testifier will be present: No
Submitted by: Michael Kitchens
Organization: Individual
E-mail: webmaster@hawaiitalks.net
Submitted on: 1/26/2012

Comments:

LATE TESTIMONY

From: mailinglist@capitol.hawaii.gov
Sent: Thursday, January 26, 2012 10:17 AM
To: ERBtestimony
Cc: aguy@aguyjohnson.com
Subject: LATE LATE Testimony for HB2288 on 1/26/2012 8:30:00 AM

Testimony for ERB 1/26/2012 8:30:00 AM HB2288

Conference room: 312
Testifier position: Oppose
Testifier will be present: No
Submitted by: andy johnson
Organization: Individual
E-mail: aguy@aguyjohnson.com
Submitted on: 1/26/2012

Comments:
Dear Legislators,

This bill violates the First Amendment and most likely the Commerce Clause of the U.S. Constitution.

In addition to its chilling effect on free speech, it's unwarranted spying on U.S. citizens, it also imposes an onerous burden on ISPs. Have you even calculated the cost in terms of simply storing these records?

Please kill this bill right away before it goes any further.

Thank you.

Craig Ellenwood
1212 Nuuanu Ave. #3912
Honolulu, HI 96817

LATE TESTIMONY

Aloha,

HB2288 should be voted down for the fact that it is an unprecedented attempt access to personal information and is a severe blow to privacy, both for individuals and business. The collection of this kind of data can be used two ways, data mining for profit and for surveillance.The government should not be allowed to record this personal information as a means of surveillance, even if it requires a warrant to access it. As the measure is written now, it does not contain any language or estimate regarding to the cost of storing such vast amount of information. How can we appropriate funds for this? Will the burden of the cost fall on the ISP, who then will pass along the cost to the consumer? The measure doesn't have any language protecting the stored data from third parties accessing the data, or requiring encryption of the stored data which in itself a serious privacy concern.

Please protect our privacy and vote NO on this measure.

Mahalo,
Craig Ellenwood
808-780-3731

LATE TESTIMONY

From: mailinglist@capitol.hawaii.gov
Sent: Thursday, January 26, 2012 10:35 AM
To: ERBtestimony
Cc: jbrown510@gmail.com
Subject: LATE LATE Testimony for HB2288 on 1/26/2012 8:30:00 AM

Testimony for ERB 1/26/2012 8:30:00 AM HB2288

Conference room: 312
Testifier position: Oppose
Testifier will be present: No
Submitted by: Jon Brown
Organization: Individual
E-mail: jbrown510@gmail.com
Submitted on: 1/26/2012

Comments:
Generally I think a lot of people are overly paranoid about privacy and sadly tech illiterate when it comes to the subject, so when I first heard about HR2288 I was skeptical that it was as onerous as some made it out to be.

Instead, I'm truly shocked anyone would pen such a horribly written bill. Seriously do you legislators even consult anyone in the tech community about this stuff?

ISPs have no business what-so-ever logging my internet destinations until AFTER they've received a valid warrant to begin doing so.

I would far rather have seen a bill that made restricted what logs ISPs could keep and how long they could be keep, than one that basically requires ISPs to operate a on-going pre-emptive wiretap of all their customers. Further HR2288 doesn't even address what hurdle law enforcement must clear to access that logged information nor restrict what the ISPs are actually allowed to do with that information or how they much securely store that information.

If this bill imposed a reasonable time frame on the history keeping, 30 days, maybe even 60 days and then provided language as to how and when that log could be accessed I'd at least feel neutral about it. As it stands you could not have written this bill more poorly.

LATE TESTIMONY

Michael J. Kitchens
91-1013 Kaiheenalu Street
Ewa Beach, HI 96706

January 26, 2012

Dear Representatives & Senators,

I'm writing you in response to the recent introduction to H.B. 2288, a bill that requires internet to keep records of all ips, domains, and host servers visited by users for two years.

This is a huge breach of privacy and is written so openly that it makes the recent SOPA/PIPA debacle look harmless in comparison. As a web developer/designer, this bill strikes me as being extremely ignorant of the basic privacy rules that have been established since the creation of the world wide web.

I am strongly opposed to this bill, and my voting will reflect as such. I highly hope that this bill will be immediately shot down. The eye of the world is currently ablaze with negativity concerning SOPA/PIPA and I would think this and any other related legislature would cast a very bad light on Hawaii, and our House/Senate as a whole if this were passed.

Mahalo,

Michael J. Kitchens
Ewa Beach Resident
Webmaster/Designer
808-847-3599

LATE TESTIMONY

From: mailinglist@capitol.hawaii.gov
Sent: Thursday, January 26, 2012 10:07 AM
To: ERBtestimony
Cc: junk@kinection.com
Subject: LATE LATE Testimony for HB2288 on 1/26/2012 8:30:00 AM

Testimony for ERB 1/26/2012 8:30:00 AM HB2288

Conference room: 312
Testifier position: Oppose
Testifier will be present: No
Submitted by: Doug Nelson
Organization: Individual
E-mail: junk@kinection.com
Submitted on: 1/26/2012

Comments:
Dear Legislators,

Please look at the fallout from SOPA and PIPA as an example of what happens when citizens and organizations band together to oppose a misguided internet bill from the government.

This bill violates the First Amendment and most likely the Commerce Clause of the U.S. Constitution.

In addition to its chilling effect on free speech, and its unwarranted spying on U.S. citizens, it also imposes an onerous burden on ISPs. Have you even calculated the cost in terms of simply storing these records?

Please kill this ridiculous bill right away before it goes any farther.

Thank you
Karen Chun
Redwood Games - Bringing you Internet games for 2 decades.

LATE TESTIMONY

From: mailinglist@capitol.hawaii.gov
Sent: Thursday, January 26, 2012 9:48 AM
To: ERBtestimony
Cc: jenadillon@gmail.com
Subject: LATE LATE Testimony for HB2288 on 1/26/2012 8:30:00 AM

Testimony for ERB 1/26/2012 8:30:00 AM HB2288

Conference room: 312
Testifier position: Oppose
Testifier will be present: No
Submitted by: Jennifer Dillon
Organization: Individual
E-mail: jenadillon@gmail.com
Submitted on: 1/26/2012

Comments:
Dear Legislators,

This awful bill represents a radical violation of privacy and opens the door to rampant Fourth Amendment violations. Additionally, it thwarts free speech, and is tantamount to spying on U.S. citizens. We continue to trade "security" for freedom in this country. What happened to land of the free, home of the brave? Please kill this terrible bill.

Sincerely,
Jennifer Dillon
145 C Auhana Road
Kihei HI 96753

LATE TESTIMONY

From: mailinglist@capitol.hawaii.gov
Sent: Thursday, January 26, 2012 9:48 AM
To: ERBtestimony
Cc: andre@americancontrols.net
Subject: LATE LATE Testimony for HB2288 on 1/26/2012 8:30:00 AM

Testimony for ERB 1/26/2012 8:30:00 AM HB2288

Conference room: 312
Testifier position: Oppose
Testifier will be present: No
Submitted by: ANDRE MAXWELL
Organization: Individual
E-mail: andre@americancontrols.net
Submitted on: 1/26/2012

Comments:
this is utter nonsense and anyone with a brain should be opposed to this.

LATE TESTIMONY

From: mailinglist@capitol.hawaii.gov
Sent: Thursday, January 26, 2012 9:36 AM
To: ERBtestimony
Cc: karen@redwoodgames.com
Subject: LATE LATE Testimony for HB2288 on 1/26/2012 8:30:00 AM

Testimony for ERB 1/26/2012 8:30:00 AM HB2288

Conference room: 312
Testifier position: Oppose
Testifier will be present: No
Submitted by: Karen Chun
Organization: Individual
E-mail: karen@redwoodgames.com
Submitted on: 1/26/2012

Comments:
Dear Legislators,

This bill violates the First Amendment and most likely the Commerce Clause of the U.S. Constitution.

In addition to its chilling effect on free speech, it's unwarranted spying on U.S. citizens, it also imposes an onerous burden on ISPs. Have you even calculated the cost in terms of simply storing these records?

Please kill this bill right away before it goes any farther.

Thank you
Karen Chun
Redwood Games - Bringing you Internet games for 2 decades.

LATE TESTIMONY

From: mailinglist@capitol.hawaii.gov
Sent: Thursday, January 26, 2012 9:32 AM
To: ERBtestimony
Cc: ljmiller@hawaii.edu
Subject: LATE LATE Testimony for HB2288 on 1/26/2012 8:30:00 AM
Attachments: testimony.txt

Testimony for ERB 1/26/2012 8:30:00 AM HB2288

Conference room: 312
Testifier position: Oppose
Testifier will be present: No
Submitted by: Lisa J Miller
Organization: Individual
E-mail: ljmiller@hawaii.edu
Submitted on: 1/26/2012

Comments: